UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/852,433	05/09/2001	Hemal V. Shah	42390P10681	4979

8791 7590 08/31/2006

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
LY, ANH VU H	

ART UNIT	PAPER NUMBER
2616	

DATE MAILED: 08/31/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/852,433	SHAH ET AL.	
	Examiner	Art Unit	
	Anh-Vu H. Ly	2616	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 June 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,6-15,18-27 and 30-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,6,7,9,10,13-15,18,19,21,22,25-27,30,31,33 and 34* is/are rejected.

7)☒ Claim(s) *8,11,12,20,23,24,32,35 and 36* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This communication is in response to applicant's amendment filed June 15, 2006.

Claims 1-3, 6-15, 18-27, and 30-36 are pending.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1, 6-7, 9-10, 13, 18-19, 21-22, 25, 30-31, 33 and 34 are rejected under 35 U.S.C. 102(e) as being anticipated by Brendel (US Patent No. 6,772,333B1).

With respect to claim 1, Brendel discloses a method comprising:

receiving a data packet from a source (col. 9, lines 3-4, the load-balancer reads incoming packets);

determining whether a session identity exists for a communication session with the source (col. 9, lines 5-7, the load-balancer will attempt to find the SSL session entry for SSL session ID in its SSL session table using SSL ID field 90);

encapsulating the received data packet in a flow header including at least two of a flow message type field, a flow option field, a source port identity field, a destination identity field,

and a session identity field in the header of the received data packet and transmitting the flow header with the received data packet to a destination if no session identity exists (col. 10, lines 5-13, when no matching SSL session ID is found in the table, the connection is for a new SSL session. The server is then assigned using the default load-balancing method, whether random, least used, or some other assignment method. The server-generated SSL session ID, which is then returned from the server in the same connection as part of the response to the encrypted client request, is stored in a new or empty entry in the table, along with the server the connection was assigned to. This implies that the client request is encapsulated and forwarded to the assigned server by the load-balancer. Herein, the addresses of the connection contains the destination address of the assigned server, e.g., MAC or IP address, col. 9, lines 10-12, and the source address and port, e.g., address and port of the load-balancer since the load-balancer connects to a plurality of servers. Therefore, the forwarded packet including at least two of source port identity field and destination identity field);

receiving the session identity from the destination using the flow header (col. 10, lines 9-13, the server-generated SSL session ID, which is then returned from the server in the same connection as part of the response to the encrypted client request, is stored in a new or empty entry in the table, along with the server the connection was assigned to. Herein, the addresses of the connection are the address of the server and address and port of the balancer); and

transmitting subsequent data packets received from the source along with the session identity to the destination (col. 10, lines 15-18, subsequent connections having the same SSL session ID will be directed to the same server, ensuring that all connections for the encrypted session are processed by the same server).

With respect to claims 6-7, 18-19, 30 and 31, Brendel discloses removing a header prior to transmitting data packets received from the destination to the source; using information in the header to transmit data packets received from the destination to the source; and wherein the information in the header comprises the source port identity (col. 8, lines 21-26, the new entry contains the SSL session ID, and the IP address of the server. The load-balancer associates the SSL session ID with the server that generated the SSL session ID, server X. The client also stores the SSL session ID and uses for all encrypted connections with the server. Herein, the destination address in the header of the packets, e.g., load-balancer's address, is removed and replaced with the address of the client, e.g., client IP address and port).

With respect to claim 9, Brendel discloses a method comprising:

receiving a data packet from a source through a network node (col. 10, lines 5-13, when no matching SSL session ID is found in the table, the connection is for a new SSL session. The server is then assigned using the default load-balancing method, whether random, least used, or some other assignment method. Herein, the server receives the packet through the load-balancer);

determining whether a session identity exists for a communication session with the source (col. 9, lines 5-7, the load-balancer will attempt to find the SSL session entry for SSL session ID in its SSL session table using SSL ID field 90);

encapsulating the received data packet in a flow header including at least two of a flow message type field, a flow option field, a source port identity field, a destination identity field, and a session identity field in the header of the received data packet and generating a session

identity if no session identity exists (col. 10, lines 5-13, when no matching SSL session ID is found in the table, the connection is for a new SSL session. The server is then assigned using the default load-balancing method, whether random, least used, or some other assignment method. The server-generated SSL session ID, which is then returned from the server in the same connection as part of the response to the encrypted client request, is stored in a new or empty entry in the table, along with the server the connection was assigned to. This implies that the client request is encapsulated and forwarded to the assigned server by the load-balancer. Herein, the addresses of the connection contains the destination address of the assigned server, e.g., MAC or IP address, col. 9, lines 10-12, and the source address and port, e.g., address and port of the load-balancer since the load-balancer connects to a plurality of servers. Therefore, the forwarded packet including at least two of source port identity field and destination identity field); and

transmitting the session identity to the network node (col. 10, lines 5-13, the server-generated SSL session ID, which is then returned from the server in the same connection as part of the response to the encrypted client request, is stored in a new or empty entry in the table of the load-balancer, along with the server the connection was assigned to).

With respect to claims 10, 22, and 34, Brendel discloses obtaining session identity from the data packet if one is included in the data packet (col. 9, lines 3-5, the load-balancer reads incoming packets and extracts SSL session ID for encrypted sessions); obtaining address information of the network node and transmitting data to the network node using address information (col. 10, lines 5-13, the server-generated SSL session ID, which is then returned

from the server in the same connection as part of the response to the encrypted client request, is stored in a new or empty entry in the table of the load-balancer, along with the server the connection was assigned to. Herein, the destination address is the address of the load-balancer).

With respect to claim 13, Brendel discloses an article of manufacture comprising:

machine-readable medium including instructions that when executed by a machine, causes the machine to perform operations (Fig. 9, client, load-balancer, and server must include medium for storing executed instructions) comprising:

receiving a data packet from a source (col. 9, lines 3-4, the load-balancer reads incoming packets);

determining whether a session identity exists for a communication session with the source (col. 9, lines 5-7, the load-balancer will attempt to find the SSL session entry for SSL session ID in its SSL session table using SSL ID field 90);

encapsulating the received data packet in a flow header including at least two of a flow message type field, a flow option field, a source port identity field, a destination identity field, and a session identity field in the header of the received data packet and transmitting the flow header with the received data packet to a destination if no session identity exists (col. 10, lines 5-13, when no matching SSL session ID is found in the table, the connection is for a new SSL session. The server is then assigned using the default load-balancing method, whether random, least used, or some other assignment method. The server-generated SSL session ID, which is then returned from the server in the same connection as part of the response to the encrypted client request, is stored in a new or empty entry in the table, along with the server the connection

was assigned to. This implies that the client request is encapsulated and forwarded to the assigned server by the load-balancer. Herein, the addresses of the connection contains the destination address of the assigned server, e.g., MAC or IP address, col. 9, lines 10-12, and the source address and port, e.g., address and port of the load-balancer since the load-balancer connects to a plurality of servers. Therefore, the forwarded packet including at least two of source port identity field and destination identity field);

receiving the session identity from the destination using the flow header (col. 10, lines 9-13, the server-generated SSL session ID, which is then returned from the server in the same connection as part of the response to the encrypted client request, is stored in a new or empty entry in the table, along with the server the connection was assigned to. Herein, the addresses of the connection are the address of the server and address and port of the balancer); and

transmitting subsequent data packets received from the source along with the session identity to the destination (col. 10, lines 15-18, subsequent connections having the same SSL session ID will be directed to the same server, ensuring that all connections for the encrypted session are processed by the same server).

With respect to claim 21, Brendel discloses an article of manufacture comprising:

a machine-readable medium including instructions that when executed by a machine, causes the machine to perform operations (Fig. 9, client, load-balancer, and server must include medium for storing executed instructions) comprising:

receiving a data packet from a source through a network node (col. 10, lines 5-13, when no matching SSL session ID is found in the table, the connection is for a new SSL session. The

server is then assigned using the default load-balancing method, whether random, least used, or some other assignment method. Herein, the server receives the packet through the load-balancer);

determining whether a session identity exists for a communication session with the source (col. 9, lines 5-7, the load-balancer will attempt to find the SSL session entry for SSL session ID in its SSL session table using SSL ID field 90);

encapsulating the received data packet in a flow header including at least two of a flow message type field, a flow option field, a source port identity field, a destination identity field, and a session identity field in the header of the received data packet and generating a session identity if no session identity exists (col. 10, lines 5-13, when no matching SSL session ID is found in the table, the connection is for a new SSL session. The server is then assigned using the default load-balancing method, whether random, least used, or some other assignment method. The server-generated SSL session ID, which is then returned from the server in the same connection as part of the response to the encrypted client request, is stored in a new or empty entry in the table, along with the server the connection was assigned to. This implies that the client request is encapsulated and forwarded to the assigned server by the load-balancer. Herein, the addresses of the connection contains the destination address of the assigned server, e.g., MAC or IP address, col. 9, lines 10-12, and the source address and port, e.g., address and port of the load-balancer since the load-balancer connects to a plurality of servers. Therefore, the forwarded packet including at least two of source port identity field and destination identity field); and

transmitting the session identity to the network node (col. 10, lines 5-13, the server-generated SSL session ID, which is then returned from the server in the same connection as part of the response to the encrypted client request, is stored in a new or empty entry in the table of the load-balancer, along with the server the connection was assigned to).

With respect to claim 25, Brendel discloses a computer system comprising:

a bus (Fig. 8, medium for connecting the session ID table 81 and receiving interface 82);

a data storage device coupled to said bus (Fig. 8, table 81); and

a processor coupled to said data storage device (Fig. 8, assigned processor 85), said processor operable to receive instructions which, when executed by the processor, cause the processor to perform a method comprising:

receiving a data packet from a source (col. 9, lines 3-4, the load-balancer reads incoming packets);

determining whether a session identity exists for a communication session with the source (col. 9, lines 5-7, the load-balancer will attempt to find the SSL session entry for SSL session ID in its SSL session table using SSL ID field 90);

encapsulating the received data packet in a flow header including at least two of a flow message type field, a flow option field, a source port identity field, a destination identity field, and a session identity field in the header of the received data packet and transmitting the flow header with the received data packet to a destination if no session identity exists (col. 10, lines 5-13, when no matching SSL session ID is found in the table, the connection is for a new SSL session. The server is then assigned using the default load-balancing method, whether random,

least used, or some other assignment method. The server-generated SSL session ID, which is then returned from the server in the same connection as part of the response to the encrypted client request, is stored in a new or empty entry in the table, along with the server the connection was assigned to. This implies that the client request is encapsulated and forwarded to the assigned server by the load-balancer. Herein, the addresses of the connection contains the destination address of the assigned server, e.g., MAC or IP address, col. 9, lines 10-12, and the source address and port, e.g., address and port of the load-balancer since the load-balancer connects to a plurality of servers. Therefore, the forwarded packet including at least two of source port identity field and destination identity field);

receiving the session identity from the destination using the flow header (col. 10, lines 9-13, the server-generated SSL session ID, which is then returned from the server in the same connection as part of the response to the encrypted client request, is stored in a new or empty entry in the table, along with the server the connection was assigned to. Herein, the addresses of the connection are the address of the server and address and port of the balancer); and

transmitting subsequent data packets received from the source along with the session identity to the destination (col. 10, lines 15-18, subsequent connections having the same SSL session ID will be directed to the same server, ensuring that all connections for the encrypted session are processed by the same server).

With respect to claim 33, Brendel discloses a computer system comprising:

a bus (Fig. 8, medium for connecting the session ID table 81 and receiving interface 82);

a data storage device coupled to said bus (Fig. 8, table 81); and

a processor coupled to said data storage device (Fig. 8, assigned processor 85), said processor operable to receive instructions which, when executed by the processor, cause the processor to perform a method comprising:

receiving a data packet from a source through a network node (col. 10, lines 5-13, when no matching SSL session ID is found in the table, the connection is for a new SSL session. The server is then assigned using the default load-balancing method, whether random, least used, or some other assignment method. Herein, the server receives the packet through the load-balancer);

determining whether a session identity exists for a communication session with the source (col. 9, lines 5-7, the load-balancer will attempt to find the SSL session entry for SSL session ID in its SSL session table using SSL ID field 90);

encapsulating the received data packet in a flow header including at least two of a flow message type field, a flow option field, a source port identity field, a destination identity field, and a session identity field in the header of the received data packet and generating a session identity if no session identity exists (col. 10, lines 5-13, when no matching SSL session ID is found in the table, the connection is for a new SSL session. The server is then assigned using the default load-balancing method, whether random, least used, or some other assignment method. The server-generated SSL session ID, which is then returned from the server in the same connection as part of the response to the encrypted client request, is stored in a new or empty entry in the table, along with the server the connection was assigned to. This implies that the client request is encapsulated and forwarded to the assigned server by the load-balancer. Herein, the addresses of the connection contains the destination address of the assigned server, e.g.,

MAC or IP address, col. 9, lines 10-12, and the source address and port, e.g., address and port of the load-balancer since the load-balancer connects to a plurality of servers. Therefore, the forwarded packet including at least two of source port identity field and destination identity field); and

transmitting the session identity to the network node (col. 10, lines 5-13, the server-generated SSL session ID, which is then returned from the server in the same connection as part of the response to the encrypted client request, is stored in a new or empty entry in the table of the load-balancer, along with the server the connection was assigned to).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 2-3, 14-15, 26, and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brendel (US Patent No. 6,772,333 B1) in view of Tal et al (US Patent No. 6,625,612 B1). Hereinafter, referred to as Brendel and Tal.

With respect to claims 2-3, 14-15, 26 and 27, Brendel discloses searching for a server in a table according to SSL session ID (col. 9, lines 5-12). Brendel does not disclose obtaining address information from the data packet; searching a table using the address information for the session identity; using the address information in a hash function to obtain a hash value; and

using the hash value to find the session identity. Tal discloses a method for obtaining the session identity from the address information. The table search operation begins with the translation of the search key, e.g., MAC address, IP address, TCP/IP session, into a (table) address by hash function HASH1(key) and into a signature by hash function HASH2(key). In some cases, the search results include session identifiers (col. 9, lines 36-47). It would have been obvious to one having ordinary skill in the art at the time the invention was made to include locating the session identity by the address information in Brendel's system, as suggested by Tal, to identify existing connections therefore, packets can be routed efficiently.

Allowable Subject Matter

4. Claims 8, 11-12, 20, 23-24, 32, and 35-36 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Response to Arguments

5. Applicant's arguments filed June 15, 2006 have been fully considered but they are not persuasive.

Applicant argues in page 15 that Brendel does not disclose transmission of the flow header and the received data packet it encapsulates to the destination if no session identity exists. Examiner respectfully disagrees. First of all, according to the specification, in page 10, lines 14-17, "Usually, at the start of each communication session the first data packet received using the transmission control protocol (TCP) is a TCP synchronizing (TCP SYN) packet. The TCP SYN packet is used to synchronize the two ends of a connection in preparation for opening a connection". This implies that the first data packet is not actual data and/or information packet

but it is a control packet or merely a request packet for requesting a new connection with a particular bit set to indicate a new connection.

Secondly, as clearly stated in the rejections of independent claims 1, 13, and 25, Brendel discloses in col. 10, lines 5-13, when no matching SSL session ID is found in the table, the connection is for a new SSL session (This implies that no session identity exists for the connection). The server is then assigned using the default load-balancing method, whether random, least used, or some other assignment method. The server-generated SSL session ID, which is then returned from the server in the same connection as part of the response to the encrypted client request, is stored in a new or empty entry in the table, along with the server the connection was assigned to (This implies that the request packet, received from the client, must be encapsulated in a flow request packet of the load balancer and forwarded to the assigned server by the load-balancer. Since it is a synchronization packet or a control packet, the whole packet contains only control information or header information. Therefore, the particular bit indicating a new connection must be encapsulated in the header section).

Conclusion

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Anh-Vu H. Ly whose telephone number is 571-272-3175. The examiner can normally be reached on Monday-Friday 7:00am - 4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Chi Pham can be reached on 571-272-3179. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

avl

CHI PHAM
SUPERVISORY PATENT EXAMINER 8/29/06